# 暗号研究の最新の動向 : 量子ワンタイムパッドの研究 (符号と暗号の代数的数理)

AUTHOR(S):

萩原, 学; 今井, 秀樹

CITATION:

萩原, 学 ...[et al]. 暗号研究の最新の動向 : 量子ワンタイムパッドの研究 (符号と暗号の代数的数理). 数理解析研究所講究録 2004, 1361: 38-46

ISSUE DATE:

2004-04

URL:

http://hdl.handle.net/2433/25256

数理解析研究所講究録 1361 巻 2004 年 38-46



# 暗号研究の最新の動向 量子ワンタイムパッドの研究

萩原 学, 今井 秀樹
Institute of Industrial Science, University of Tokyo,
4-6-1 Komaba, Meguro-ku Tokyo, Japan
E-mail: {manau, imai}@{imailab.iis, iis}.u-tokyo.ac.jp

## 1 導入

タイトルは“暗号研究の最新の動向”とあるが、テーマを絞って量子暗号、とくに量子ワンタイムパッドの研究について紹介する。量子暗号の研究は近年盛んに行われていて、量子鍵配送の装置は、幾つかの国で発売もはじまっているから、最新の暗号研究の一つだと思ってよいと考える。ところで、量子暗号の研究には量子力学の幾つかの知識が必要とされる。この草稿では最低限必要な知識を紹介していく。全く量子力学の勉強をしたことがなくても、この寄稿集で書かれている量子暗号の内容（量子ワンタイムパッドだけでなく、量子誤り訂正符号や量子鍵配送など）が読めるように、§2 と §3 にて量子情報理論に必要な知識を少しだけまとめることに努力した。本題である量子ワンタイムパッドに関しては §4 で定義や問題が記述される。ここでの問題は、通常、量子情報理論的な研究方法で進められるものであり、また紹介されている問題も既に解決済みのものであることを注意しておく。しかし、量子情報理論を用いず、簡単な数学で別の証明を与える (§5)。

## 2 準備 1 ベクトルによる量子状態の記述

**Axiom.** $n$ を 2 以上の自然数とする。量子状態 $|\phi\rangle$ とは、$\mathbb{C}^n$ の元（ベクトル）のうち、（普通の内積での）長さが 1 であるものを意味する。量子状態は、スカラー倍しても同一の状態だとみなす。$V_1 \oplus V_2 \oplus \cdots \oplus V_d$ を $\mathbb{C}^n$ の直交分解だとする。このとき、量子状態 $|\phi\rangle$ を $V_1, V_2, \ldots, V_d$ によって観測する

と、$|\phi\rangle = \oplus_{i=1}^{d}|\phi_i\rangle$ ($|\phi_i\rangle \in V_i$) とかけば、確率 $||\phi_i\rangle|^2$ で $|\phi\rangle$ は $|\phi_i\rangle$ になって、$V_i$ の元だということがわかる。

**Example 2.1.** $n = 2$ とする。また、$\mathbb{C}^2$ の正規直交基底を一つ選びそれを $\{|0\rangle, |1\rangle\}$ と書く。

$|0\rangle$ を $\langle|0\rangle\rangle \oplus \langle|1\rangle\rangle$ で観測すると、確率 1 で $|0\rangle$ になる。

続いて、$\langle\frac{|0\rangle+|1\rangle}{\sqrt{2}}\rangle \oplus \langle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\rangle$ で観測すると、確率 1/2 で $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$、確率 1/2 で $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ になる。この場合、直交分解が一次元に分解されているので、どの状態であるかもわかる。

さらに続いて、$\langle\frac{|0\rangle+|1\rangle}{\sqrt{2}}\rangle \oplus \langle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\rangle$ で観測すると、確率 1 で直前と同じ状態になる。

さらに、$\langle|0\rangle\rangle \oplus \langle|1\rangle\rangle$ で観測すると、確率 1/2 で $|0\rangle$ になり、確率 1/2 で $|1\rangle$ になる。

**Axiom.** 量子状態 $|\phi\rangle \in \mathbb{C}^n$ に対して、$\phi\rangle$ がどんな状態であるか知らなくてもユニタリ変換 $x \in U(\mathbb{C}^n)$ を走作（作用）させることができる。

**Example 2.2.** 情報源 $S$ から量子メモリ（量子状態を保管する道具）$M$ に量子状態を送るとする。途中、ユニタリ変換 $x$ が作用されるとする。$S$ からは $|0\rangle$ と $|1\rangle$ のどちらかが確率 1/2 で一つ送られるとしよう。このとき、$x = I$（単位行列）ならば $M$ には確率 1/2 で $|0\rangle$ か $|1\rangle$ のどちらかが保管される。また、$x = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$ とすると、$M$ には確率 1/2 で $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ か $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ のどちらかが保管される。

## 3 準備 2 行列による量子状態の記述

**Axiom.** 情報源 $S$ が量子状態 $|\phi_j\rangle$ を確率 $p_j$ で発生させるとする。このことを $\rho := \sum_j p_j|\phi_j\rangle\langle\phi_j|$ で表す。ここで、$\langle\phi|$ は $|\phi\rangle$ の転置共役を表す。$\rho$ のことも量子状態と呼ぶ。（この条件は、行列環 $M_n(\mathbb{C})$ の元 $\rho$ でトレースが 1 であり、その転置共役 $\rho^\dagger$ がそれ自身と等しく、また非負定値であるもの全体である。）$V_1 \oplus V_2 \oplus \cdots \oplus V_d$ を $\mathbb{C}^n$ の直交分解だとし、それぞれの空間 $V_i$ への射影子を $P_i$ とする。このとき、量子状態 $\rho$ を $V_1, V_2, \ldots, V_d$ によって観測すると、$\rho$ は確率 $\mathrm{Trace}(P_i\rho P_i^\dagger)$ で $\frac{1}{\mathrm{Trace}(P_i\rho P_i^\dagger)} P_i\rho P_i^\dagger$ になる。

**Example 3.1.** $n = 2$ とする。$\rho = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ を射影子 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ で観測すると、$\rho$ は $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ のままである。

続いて射影子 $\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ で観測すると、$\rho$ は確率 $1/2$ で $\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$、確率 $1/2$ で $\frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ になる。

**Axiom.** 量子状態 $\rho \in M_n(\mathbb{C})$ に対して、$\rho$ が何か知らなくてもユニタリ変換 $x \in U_n(\mathbb{C})$ を作用させることができ、その結果 $x\rho x^\dagger$ になる。

**Example 3.2.** 情報源 $S$ から量子メモリ $M$ に対し、量子状態 $|0\rangle, |1\rangle$ がそれぞれ確率 $1/2$ で送られるとする。このとき、途中でどんな $x \in U_2(\mathbb{C})$ を作用させても、$M$ にある量子状態は $\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ である。

**Proposition 3.3.** 量子状態 $\rho = \frac{1}{n}I$ を $V_1 \oplus V_2 \oplus \cdots \oplus V_d$ で観測したとき、確率 $\frac{\dim V_i}{n}$ で $\frac{n}{\dim V_i}P_i$ になる。ここで、$P_i$ は $V_i$ への射影子である。

*Proof.* 直接計算で確かめられる。 □

**Axiom.** 量子状態 $\rho$ に対し、ユニタリ変換 $x_1, x_2, \ldots, x_k$ がそれぞれ確率 $p_1, p_2, \ldots, p_k$ で作用すると $\rho$ は $\sum_i p_i x_i \rho x_i^\dagger$ になる。

# 4 量子ワンタイムパッド

ある量子通信路があり、そこを量子状態が流れているとする。どんな量子状態が流れているかはわからないが、それを暗号化して送るアルゴリズムを考える。暗号化する方法として、量子状態にユニタリ変換を作用させるという方法をとることにする。同じユニタリ変換 $x$ だけを作用させていたら、盗聴者は $x^{-1}$ を作用させることで量子状態のもつ情報が奪われてしまう。そこで、幾つかのユニタリ変換 $x_1, x_2, \ldots, x_r$ を準備しておき、それぞれを適当に振り分けて作用させることにする。いつ、どのユニタリ変換を作用させたかは、暗号化したものだけが記憶しておくことにする。この単純な方法で、盗聴者がまったく情報を得られないような暗号化ができるようにしたい。このことを式で書いたものが、次である。

**Definition.** $X$ を $U_n(\mathbb{C})$ の有限部分集合、$p_X$ を $X$ 上の確率分布とする。$(X, p_X)$ が量子ワンタイムパッドであるとは、任意の量子状態 $\rho \in M_n(\mathbb{C})$ に対し

$$\sum_{x \in X} p_x x \rho x^\dagger = \frac{1}{n} I$$

となることである。

**問題 4.1.** $\#X$ の最小値はいくつになるか。*(答えは Corollary 5.2 を参照。)* また、$\#X$ による $p_X$ への制約はあるか。(答えの一つとして *Corollary 5.4* を参照。)

**Example 4.2.** $X$ が群をなしているとし、またこの行列表現により既約であるとする。また、$p_X$ が一様分布だとする。このとき、$(X, p_X)$ は量子ワンタイムパッドである。

*Proof.* Shur の補題から直ちにわかる。 □

**Example 4.3.** *Weyl* の誤り基底 $X$ と一様分布 $p_X$ のペアは量子ワンタイムパッドである。つまり、

$$X = \{x^i y^j | 0 \leq i, j < n\}$$

であり、ここで $x = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \cdots & & \\ & & & 0 & 1 \\ 1 & & & & 0 \end{pmatrix}, y = \begin{pmatrix} 1 & & & & \\ & \omega & & & \\ & & \omega^2 & & \\ & & & \ddots & \\ & & & & \omega^{n-1} \end{pmatrix}$

であり、$\omega$ は 1 の原始 $n$ 乗根である。

*Proof.* $G$ を $X$ の生成する群とすると

$$G = \{\omega^h x^i y^j | 0 \leq h, i, j < n\}$$

が従う。また、この行列表現は既約表現。

$$\sum_{0 \leq i,j < n} \frac{1}{n^2} (x^i y^j) \rho (x^i y^j)^\dagger = \sum_{0 \leq h,i,j < n} \frac{1}{n^3} (\omega^h x^i y^j) \rho (\omega^h x^i y^j)^\dagger = I$$

□

**Example 4.4.** 行列環 $M_n(\mathbb{C})$ に対し、内積 $\langle , \rangle_{tr} : M_n(\mathbb{C}) \times M_n(\mathbb{C}) \to \mathbb{C}$ を $\langle A, B \rangle_{tr} = \frac{1}{n} \mathrm{Trace}(AB^\dagger)$ と定義する。ここで、$A, B \in M_n(\mathbb{C})$ である。

$X \subset U_n(\mathbb{C})$ が $\langle A, B \rangle_{tr}$ に関して正規直交基底であり、$p_X$ が一様分布であるならば、$(X, p_X)$ は量子ワンタイムパッドである。

*Proof.* この例は良く知られたもので、証明はここでは省略する。後に、Theorem5.1 と Proposition5.3 から示される。 □

# 5 要素ベクトル

**Definition.** $X$ を $U_n(\mathbb{C})$ の有限部分集合とし、$p_X$ を $X$ 上の確率分布とする。いま、$\mathbb{C}^X$ と書いて、$\#X$ 次元複素ベクトル空間でそのインデックスに $X$ の元をもつものとする。$(X, p_X)$ に対して、$n^2$ 個の $\mathbb{C}^X$ の元を以下のように対応させる。$1 \leq a, b \leq n$ に対し、$\mathbf{x}_{a,b} \in \mathbb{C}^X$ の $x$ 成分を、$x$ の $(a,b)$-成分 $x_{a,b}$ と $\sqrt{p_x}$ の積 $\sqrt{p_x}x_{a,b}$ とする。この $n^2$ 個のベクトルを**要素ベクトル**と呼ぶ。

つまり、先の問題 4.1 を解くために、$(X, p_X)$ の構造を、要素ベクトルの構造に置き換え、$\#X$ の最小値を、要素ベクトルの次元の問題として解くわけである。また、要素ベクトルに対して内積 $\langle , \rangle_n$ を次のように定義する。

$$\langle \mathbf{x}_{a,b}, \mathbf{x}_{c,d} \rangle_n := \frac{1}{n} \sum_{x \in X} x_{a,b} x_{c,d}^{\dagger}$$

である。これは、複素ベクトルとしての普通の内積を $1/n$ 倍してものに等しい。

**Theorem 5.1.** $(X, p_X)$ が量子ワンタイムパッドであることの必要十分条件は、対応する要素ベクトルが内積 $\langle , \rangle_n$ において互いに直交し、かつ全て同じ長さ 1 となることである。

*Proof.* $X = \{x_1, x_2, \ldots, x_r\}$ とし、$x_i$ に対する確率を $p_i$ と書くことにする。まず、必要条件であることを示す。$1 \leq h, k \leq n$ に対して、$E_{h,k} := (\delta_{(a,b)=(h,k)})_{a,b}$ とおく。いま、$E_{t,t}$ は量子状態である。ここで、簡単に

$$\sum_{1 \leq s \leq r} p_s X_s E_{t,t} X_s^{\dagger} = (\langle \mathbf{x}_{a,t}, \mathbf{x}_{b,t} \rangle_n / n)_{a,b}$$

が確かめられる。であるから、

$$\langle \mathbf{x}_{a,t}, \mathbf{x}_{b,t} \rangle_n = \delta_{a,b}.$$

が必要条件であることがわかった。ここで、$\delta$ はクロネッカーのデルタである。

次に、$1 \leq h < k \leq n$ に対して、

$$\rho_{h,k}^{i} := 1/2(E_{h,h} + E_{k,k} + iE_{k,h} - iE_{h,k}),$$

$$\rho_{h,k}^{1} := 1/2(E_{h,h} + E_{k,k} + E_{k,h} + E_{h,k})$$

と、おく。やはり、$\rho_{h,k}^{i}, \rho_{h,k}^{1}$ もまた量子状態である。

そこで計算すると、

$$\sum_{1\le s\le r} p_s X_s \rho^i_{h,k} X_s^\dagger$$
$$= \frac{1}{2n}(\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,h}\rangle_n + \langle \mathbf{x}_{a,k}, \mathbf{x}_{b,k}\rangle_n - i\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n + i\langle \mathbf{x}_{a,k}, \mathbf{x}_{b,h}\rangle_n)_{a,b}$$
$$= \frac{1}{2n}(2\delta_{a,b} - i\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n + i\langle \mathbf{x}_{a,k}, \mathbf{x}_{b,h}\rangle_n)_{a,b}$$

であり、また

$$\sum_{1\le s\le r} p_s X_s \rho^1_{h,k} X_s^\dagger$$
$$= \frac{1}{2n}(\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,h}\rangle_n + \langle \mathbf{x}_{a,k}, \mathbf{x}_{b,k}\rangle_n + \langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n + \langle \mathbf{x}_{a,k}, \mathbf{x}_{b,h}\rangle_n)_{a,b}$$
$$= \frac{1}{2n}(2\delta_{a,b} + \langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n + \langle \mathbf{x}_{a,k}, \mathbf{x}_{b,h}\rangle_n)_{a,b}$$

となる。

よって、$\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n - \langle \mathbf{x}_{a,k}, \mathbf{x}_{b,h}\rangle_n = 0$ かつ $\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n + \langle \mathbf{x}_{a,k}, \mathbf{x}_{b,h}\rangle_n = 0$ を得た。

このように、$1 \le h < k \le n$

$$\langle \mathbf{x}_{a,h}, \mathbf{x}_{b,k}\rangle_n = 0$$

が成り立つ。

任意の量子状態は、$E_{t,t}, \rho^i_{h,k}, \rho^1_{h,k}$ の一次結合で書くことができる。よって、必要条件である。

十分性を示すには、いままでの議論を逆にたどればよい。 □

以下の結果は量子情報理論的な証明が既に知られているものだが、今回、別の証明を Theorem 5.1 から与えた。

**Corollary 5.2 ([2], [3]).** 量子ワンタイムパッド $(X, p_X)$ において、$\#X \ge n^2$ が成り立つ。

*Proof.* 一般に、もし $\mathbb{C}^r$ の元が $t$ 個あり、直交しているとき、$r \ge t$ が従う。いま、Theorem 5.1 でのベクトルの数は $t = n^2$ であった。よって、$r = |X| \ge n^2$ が従う。 □

先にあげた Example 4.4 が量子ワンタイムパッドであることの証明をしよう。次の Proposition を示す。

**Proposition 5.3.** $X = \{X^k\}$ を $U(\mathcal{H})$ を複素ベクトル空間と見たときの基底とする。また、$p_X$ を $X$ 上の確率とする。$X$ が *Trace* 内積で正規直交基底であり $p_X$ が一様分布であることの必要十分条件は、$(X, p_X)$ の要素ベクトルが $\langle , \rangle_n$ によって正規直交基底となることである。

*Proof.* $\{x_{a,b}\}_{1 \leq a,b \leq n^2}$ を要素ベクトルとする。いま、サイズ $n^2 \times n^2$ である次の行列 $U$ を以下のように定義する。

$$U = \begin{pmatrix} x_{1,1} \\ x_{1,2} \\ \cdots \\ x_{1,n^2} \\ x_{2,1} \\ x_{2,2} \\ \cdots \\ x_{n^2,n^2} \end{pmatrix}$$

すると簡単な計算により、

$$UU^\dagger = (x_{a,b}x_{c,d}^\dagger)_{i=(a-1)n+b, j=(c-1)n+d} = 1/n(\langle x_{a,b}, x_{c,d} \rangle_n)_{i=(a-1)n+b, j=(c-1)n+d}$$

が従うことがわかる。一方、

$$U^\dagger U = (\sqrt{p_i p_j}\mathrm{Tr}(X_i X_j^\dagger))_{i,j} = (n\sqrt{p_i p_j}\langle X_i, X_j \rangle_{Tr})_{i,j}$$

も成立する。

もし要素ベクトルが $\langle , \rangle_n$ によって正規直交基底となっているとする。このとき、

$$UU^\dagger = \frac{1}{n} I_{n^2}$$

が従う。このように、$nU^\dagger$ は $U$ の逆行列である。であるから、

$$U^\dagger U = \frac{1}{n} I_{n^2}$$

が従う。よって、

$$n\sqrt{p_i p_j}\langle X_i, X_j \rangle_{Tr} = \delta_{i,j}/n$$

が成り立つ。つまり、$X$ は直交基底である。また、ユニタリ性より、$\langle X_i, X_i \rangle_{Tr} = 1$ が成立する。このように、$X$ は Trace 内積により正規直交基底である。もっと詳しく、$p_i = 1/n^2$ も成立している。

逆に、$X$ を Trace 内積による正規直交基底とし、$p_X$ を一様分布とする。すると、

$$U^\dagger U = 1/nI_{n^2}$$

が成立する。また、

$$UU^\dagger = 1/nI_{n^2} = (x_{a,b}x_{c,d}^\dagger)_{i=(a-1)n+b,j=(c-1)n+d}$$

が成り立つ。このように、要素ベクトルは正規直交基底である。 □

**Corollary 5.4.** $(X, p_X)$ が最適量子ワンタイムパッドであるとする。このとき、$p_X$ は一様分布である。

*Proof.* Proposition 5.3 と Theorem 5.1 から明らか。 □

# 6 最後に

量子暗号の一つとして、量子ワンタイムパッドを紹介し、幾つかの性質を示した。今回示した性質は、情報理論からアプローチされてきたものだった。それに対し、線形代数などの数学を用いた別証を与えてみた。

量子ワンタイムパッドに関して、気になることはいろいろある。たとえば、"一様分布でない確率分布 $p_X$ で量子ワンタイムパッドを構成すると $\#X$ の最小値はいくつになるだろうか"、また、情報源 $S$ が特定の量子状態しか出さなかった場合に、$\#X$ の最小値はどう変化するのか。実はあまりわかっていないのが現状である。

今回の内容に興味を覚えた場合は、参考文献にあげたものから研究を進めることができる。また、e-Print archive の quant-ph に最新の研究成果がアップロードされるので、こまめにチェックするとよい。量子ワンタイムパッドは、Private Quantum Channels の特別な場合として研究されていることもあることを注意しておく。また、Trace 内積で正規直交という条件は "Unitary Error Basis" という言葉を用いられることが多い。これは、量子誤り訂正符号や量子高密度符号化、量子テレポーテーションの理論でも有用な道具である。これらに興味を広げて研究を進めるのもよい方法だと思う。

**Acknowledgments.** This work was supported by the project on "Research and Development on Quantum Cryptography" of Telecommunications Advancement Organization as part of the programme "Research and Development on Quantum Communication Technology" of the Ministry of Public Management, Home Affairs, Posts and Telecommunications of Japan.

# References

[1] Andreas Klappenecker, Martin R¨
Error Bases, arXiv:quant-ph/0010082.

[2] Michele Mosca, Alain Tapp and Ronald de Wolf, Private Quantum Channels and the Cost of Randomizing Quantum Information, arXiv:quant-ph/0003101.

[3] P. Oscar Boykin and Vwani Roychowdhury, Optimal Encryption of Quantum Bits, arXiv:quant-ph/0003059.

[4] R. F. Werner, All Teleportation and Dense Coding Schemes, arXiv:quant-ph/0003070.